单向网络安全设备的分析与证明 *

王雪健，赵国磊，常朝稳，王瑞云

(中国人民解放军信息工程大学，郑州 450001)

摘 要：单向网络安全设备是不同密级间网络信息传输的主要安全设备。为保证单向网络安全设备内部的安全性和通信系统的安全性，分析了单向网络安全设备的安全需求，提出无干扰模型形式化建模，用数学归纳法证明单向网络安全设备安全需求与形式化策略规约的一致性；并针对单向网络安全设备存在的安全隐患进行分析与讨论，总结出更加完善安全策略，确保信息安全。这为单向网络安全设备的安全性设计提供了一定的借鉴意义。

关键词：单向网络安全设备；形式化；无干扰模型；安全策略；数学归纳法

中图分类号：TP309.   doi: 10.3969/j.issn.1001-3695.2017.11.1004

Analysis and proof of one-way network safety equipment

Wang Xuejian, Zhao Guolei, Chang Chaowen, Wang Ruiyun

(*PLA Information Engineering University*, *Zhengzhou* 450001, *China*)

Abstract: One-way network safety equipment is the major security equipment of information transmission between different classified levels. To ensure the safety equipment within the one-way network security and the security of the communication system , this paper analyzed the security requirements of one-way network security equipment, presented noninterference model, and proved the consistency of one-way network security equipment safety requirements and formal specification with mathematical induction. It analyzed and discussed the safety hazards of one-way network safety equipment, and the security policy was more perfect for information security. It plays certain referential significance on security design of one- way safety equipment.

Key Words: one-way network safety equipment; formalization; noninterference; security policies; mathematical induction

0 引言

近年来，随着网络间流量规模增大，计算机遭受攻击的风险不断增高，传统的安全手段（如防火墙[1]、入侵检测[2−3]）越来越难处理其相应的攻击。为抵御这些新的安全威胁、减少系统存在的漏洞，必须增加新的安全设备或重新设计网络构架[4]以提供更多的安全功能。不同级别网络间信息的双向交互，使得安全设备内部通信系统[5]信息交互的复杂度进一步增大，由此引入单向网络安全设备[6]来确保低保密级别网络到高保密级别网络的信息流动安全性。在发送端、单向网络安全设备、接收端所构成的通信系统中，发送端仅发送信息到单向网络安全设备中，不接受任何数据，保证低保密级别安全域中的计算机或存储设备向高保密级别安全域中计算机单向、安全、快速地数据传输，即使高保密级别的计算机被非法控制，文件数据也不能向低保密级别的存储设备进行数据传输。常见的单向网络安全设备有单向网闸、单向性安全网关[7]等。

今天，关于单向网络安全设备的安全性分析及证明方法已有很多，但都缺乏自身性、理论性基础。单向网络安全设备的安全需求由自身内部的安全策略[8]所决定，安全策略模型的形式化分析、设计和验证正是当今形式化分析研究领域的热点问题。经典的形式化信息安全策略模型有信息流模型[9]、BLP 模型[10]、无干扰安全模型[11]等。由于读、写等操作背后隐藏的信息流并不像字面上那样明确,为了排除隐蔽信道[12]还需要增加很多限制，但无干扰安全模型不仅能对其安全性进行验证,还可以指导设计者对信息流的判断（以一种更具有包容性的“读”“写”实现信息在传递中的安全性）。所以本文选择无干扰安全模型对单向网络安全设备的策略进行安全性分析，并证明其功能规约与安全模型策略间的一致性。

文章介绍了单向网络安全设备,同时建立出它的抽象模型;介绍关于无干扰的相关研究，并且根据 Goguen 和 Meseguer 无干扰模型[13]将所述的抽象模型进行形式化转变，提出相应的安全策略；用数学归纳法[6]验证形式化后的模型在安全策略下满

基金项目：面向用户的可信云计算环境安全研究基金资助项目（61572517）

作者简介：王雪健（1993-），男，硕士研究生，主要研究方向为信息安全、形式化验证（1368154434@qq.com）；赵国磊（1979-），男，讲师，博士，主要研究方向为信息安全、形式化验证；常朝稳（1966-），男，教授，博导，博士，主要研究方向为信息安全；王瑞云（1992-），女，硕士研究生，主要研究方向为信息安全.

足其需求与规约的一致性；讨论了隐通道[14]的存在情形，并提出相应策略调整以确保整体通信系统的安全；最后给出关于单向网络安全设备的分析结论和下一步研究重点。

1 单向网络安全设备的抽象模型

单向网络安全设备常常被应用在涉密和非涉密、高安全和低安全级别网络边界，并在不同级别网络信息交互中确保高级别网络数据的机密性和完整性，如图 1 所示。

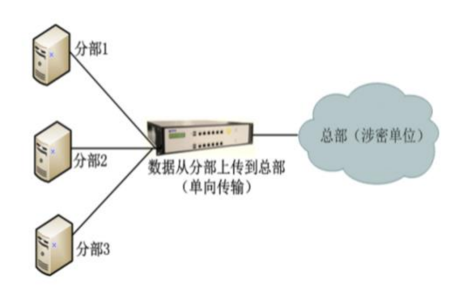


图 1 单向网络设备应用场景

一个单向网络安全设备控制着来自低级别网络的输入信息，且在单向网络安全设备内包含一系列通信模块分析和传递这些信息，使得低密级网络域中主/客体(如图中分部)能够通过单向网络安全设备传递信息到高密级网络中(如图中总部)。但在这一过程中信息的传递是否真的安全，需要进一步考察与分析，由此引入安全模型的概念。

安全模型[13]的目的是精确地描述系统的安全需求，具有如下几个特点：它是精确、无二义性的；是简单、抽象的；具有一般性，仅涉及安全性质，不过分限制系统的功能及其实现；是安全策略的一个清晰的表达方式。

本文研究的单向网络安全设备与低保密级别网络域 L_{-D} 和接高保密级别网络域 H_{-D} 所构成的通信系统为确定性同步系统，抽象结构的逻辑组成如图 2 所示。

图 2 的逻辑结构表示信息由低保密级别网络域 L_{-D} 流入高保密级别网络域 H_{-D} 的情形，由低保密级别网络域 L_{-D} 进入的信息被单向网络安全设备内部通信模块处理后进入高保密级别网络域 H_{-D}。

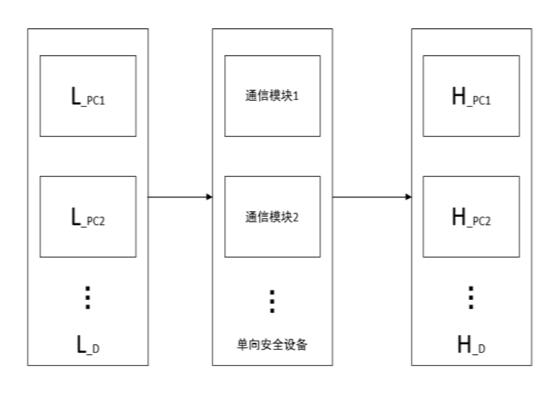


图 2 通信系统逻辑结构

为确保单向网络安全设备对 L_{-D} 到 H_{-D} 的信息过滤，模型需要满足以下两个安全需求：

a)过滤性。经过单向网络安全设备传递到其他网域的信息必须经过单向设备内部的通信模块过滤；

b)单向性。单向网络安全设备内部任意通信模块间信息的传递是单向的。

由此，下面以单向网络安全设备内部信息简单的串行传递（图 3）为例，作出如下功能规约：图 3 中任意模块中高级别的主体执行该模块中命令时对低级别主体满足无干扰性。

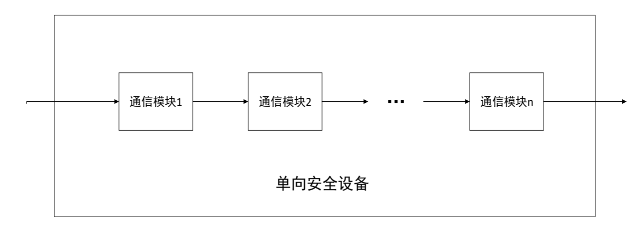


图 3 内部通信模块串行结构图

为形式化证明出单向网络安全设备安全策略的安全性，本文首先用无干扰模型形式化的描述出单向网络安全设备模型，其次再证明该单向网络安全设备在其模型策略下是安全的。

1.1 无干扰的相关研究

早期由 Goguen 和 Meseguer 提出信息流的无干扰思想，随后出现多种无干扰安全模型[14-16]，直到 1992 年，Rushby 对 Goguen 和 Meseguer 的无干扰模型[13]进行改进，修正其中几处错误，使其更合理并容易理解，无干扰模型也趋于成熟。

无干扰模型提出一种根据“干扰”来分析安全的新视角。本质上，如果系统内组与组之间的主体不互相干扰，那么这个系统就是安全的。显然，这种比传统意义上的写操作更具包容性[17]，能够更简单地表达策略和模型。Goguen 和 Meseguer 由此来定义安全策略模型。

1.2 无干扰策略模型

无干扰策略模型的基本定义：首先将一个系统 X 视为一个状态机，它包含一个主体的集合 S，（$S=\{s_1,s_2,\ldots\}$），一个状态集合 Q，($Q=\{\delta_0,\delta_1,\ldots\}$),一个状态命令集合 C,($C=\{c_1,c_2,\ldots\}$),一个输出集合 O，（$O=\{o_1,o_2\ldots\}$）。（实际上执行命令主体的等级影响了这条实际被执行的命令，所以这里用一个命令集合 Z，（$Z=\{z_1,z_2,\ldots\}$)中的一个状态转换命令集合 $C=S\times Q$ 列出)。

定义 1 状态转换函数 $tra:C\times Q\rightarrow Q$，描述了在状态 δ 下执行命令 c 的效果表。输出函数 $out:C\times Q\rightarrow O$ 描述了在状态 δ 下执行命令 c 的机器输出。

定义 2 设 $tra^*(c_s,\delta_i)$ 某系统的一个状态转换序列（c_s 为一个命令序列，i 为正整数），$out^*(c_s,\delta_i)$ 是对应的输出。那么 $out^{'}(s,c_s,\delta_i)$ 是在中 $out^*(c_s,\delta_i)$ 输出的一个集合，它代表主体 s 被授权可见且与其在 $out^*(c_s,\delta_i)$ 中输出顺序一致的输出集合（其中 i 为自然数），即：函数 $out^{'}(s,c_s,\delta_i)$ 表示只是从输出中删除没有授权 s 可见的输出后，所得到的输出序列。

该定义表达出：由于安全策略限制了 s 对这些输出的访问，

s 可能会看不到所有的输出。然而 s 也可能不会拥有所有命令的知识，所以还需如下定义。

定义 3　设 $G \subseteq S$ 是一个主体集合，$A \subseteq Z$ 是一个命令集合。定义 $\pi_G(c_s)$（清除函数）为从 c_s 中删除所有符合 $s \in G$ 的 (s,z) 元素所得的子序列。定义 $\pi_A(c_s)$ 为从 c_s 中删除所有符合 $z \in A$ 的 (s,z) 元素所得的子序列。定义 $\pi_{G,A}(c_s)$ 为从 c_s 中删除所有符合 $s \in G$ 且 $z \in A$ 的 (s,z) 元素所得的子序列。

直观上，如果任何用户可见的输出集都与该用户可见的输入集相关，那么这个系统就是安全的。以下定义将此形式化为“无干扰性”。

无干扰性定理　设 $G, G' \subseteq S$ 是两个不同主体集合，$Z_1 \subseteq Z$ 是一个命令集合。G 中的用户在运行 Z_1 中的命令是不干扰 G' 中的用户（记为 $Z_1, G :| G'$），当且仅当对于所有由 C^* 中元素组成的序列 c_s 和所有的 $s \in G'$，有：$out'(s, c_s, \delta_i) = out'(s, \pi_{G,Z_1}(c_s), \delta_i)$。

1.3　无干扰形式化描述

现在基于 2.1 节无干扰模型形式化描述出单向网络安全设备模型及其策略。

将图 3 中模型视为一个系统 $X = (S,Q,O,Z)$，即：

S：一个主体的集合 $\{s_{l_1}, s_{l_2}, \ldots, s_{l_n}\}$（$n$ 为正整数）；Q:一个状态集合 $\{\delta_0, \delta_1, \ldots\}$，其中 δ_0 为系统初态且 $\delta_0 = \{(s_{l_1},\delta_0)(s_{l_2},\delta_0),\ldots,(s_{l_n},\delta_0)\}$；$O$:一个输出集合 $\{o_1, o_2, \ldots\}$；Z:一个命令集合 $\{z_1, z_2, \ldots\}$，其中定义状态转换命令为 $C = S \times Q$，用 $\{(s_{l_i}, c_1), (s_{l_i}, c_2), \ldots\}$ 表示。

若典型安全设备内部通信模块 1 为外网通信模块，通信模块 2、4 为过滤器模块，通信模块 3 为加密模块，通信模块 5 为内网通信模块，将图 3 形式化表示成如图 4 所示。

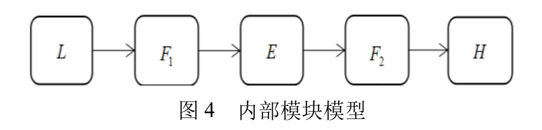


图 4　内部模块模型

L 表示外网通信模块，模块内任意主/客体状态记为 δ_0；F_1, F_2 分别表示两个过滤器模块，模块内任意主/客体状态分别记为 δ_1、δ_3；E 表示据加解密模块，模块内任意主/客体状态记为 δ_2；H 表示内网通信模块，模块内任意主/客体状态记为 δ_4。当整个网关内部有两个主/客体 s_{l_1}, s_{l_2} 时，令其执行状态转换的命令域分别为 $dom(c_{s_{l_1}})$，$dom(c_{s_{l_2}})$。

图 4 中涉及的信息传递的状态转换如图 5 所示。

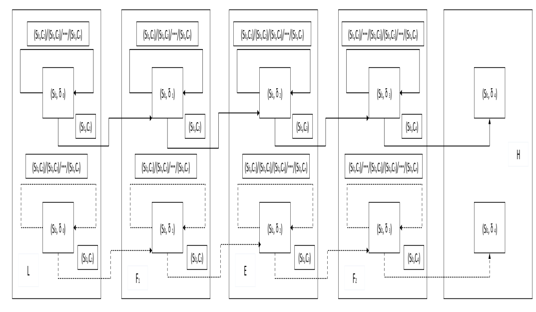


图 5　内部模块信息传递图

由 2.1 节中定义 1、2 可类似定义：

状态转换函数 $tra: C \times Q \to Q$，描述了在状态 δ 下执行命令 c 的效果。对于主体 s_{l_1}，其中实际有效的状态转换为：$tra((s_{l_1}, c_1), \delta_0) = \delta_1$，$tra((s_{l_1}, c_2), \delta_1) = \delta_2$，$tra((s_{l_1}, c_3), \delta_2) = \delta_3$，$tra((s_{l_1}, c_4), \delta_3) = \delta_4$，其余状态转换命令皆未使状态发生转变。

输出函数 $out: C \times Q \to O$，描述了在状态 δ 下执行命令 c 的机器输出（此时该状态下主/客体的个数）。

函数 $out'(s_{l_1}, c_s, \delta_i)$ 表示只是从输出中删除没有授权 s_{l_1} 可见的输出后，所得到的输出序列。

清除函数与定义 3 中一致。

2　需求与形式化策略规约的一致性证明

现在用形式化方法和数学工具证明此时单向网络安全设备的策略满足无干扰性，由无干扰模型自身限制，现考虑不同级别信息传递的情形（相同级别信息见第 4 章）。

a) 对于模块 L 内部，若 s_{l_1}, s_{l_2} 是两个不同的主/客体且 $level(s_{l_1}) < level(s_{l_2})$，状态转换如图 6 所示。

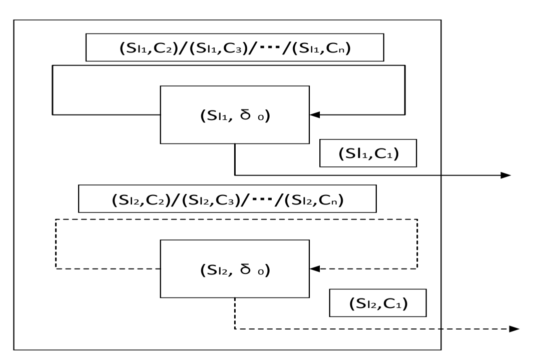


图 6　模块 L 内信息流动

显然模块内部主体 s_{l_1} 和 s_{l_2} 的命令是隔离的，有 $dom(c_{s_{l_1}}) \cup dom(c_{s_{l_2}}) = Z$ 并且 $dom(c_{s_{l_2}}) = Z_1$，$dom(c_{s_{l_1}}) \cap dom(c_{s_{l_2}}) = \varnothing$。由无干扰性定理可知:

$$out'(s_{l_1}, c_s, \delta_i) = out'(s_{l_1}, \pi_{s_{l_2}, dom(c_{s_{l_2}})}(c_s), \delta_i)。$$

举例　由于模块 L 内部主/客体 s_{l_1} 所能观察的状态仅为 δ_0，所以仅需考虑上式 $i=0$ 的情况。不失一般性，令在系统初态下，主体 s_{l_1} 在自身权限内观察到 δ_0 的个数为 m_1（m_1 取自然数）个，即 $out(s_{l_1}, c_0, \delta_0) = m_1$（$c_0$ 为空命令）；同理，对主体 s_{l_2} 有 $out(s_{l_2}, c_0, \delta_0) = m_2$。

取 $c_s = (s_{l_1}, c_i)(s_{l_2}, c_1)(s_{l_1}, c_1)(s_{l_2}, c_j)$（其中 i，j 为正整数且 i，$j \neq 1$）。

当系统在模块 L 中执行 c_s 命令序列后，则 $out'(s_{l_1}, c_s, \delta_0) = (m_1)(m_1 - 1)$，显然 $dom(c_{s_{l_2}}) \subseteq Z$，$\pi_{s_{l_2}, dom(c_{s_{l_2}})} = (s_{l_1}, c_i)(s_{l_1}, c_1)$，$out'(s_{l_1}, \pi_{s_{l_2}, dom(c_{s_{l_2}})}(c_s), \delta_0) = (m_1)(m_1 - 1)$，则：$out'(s_{l_1}, c_s, \delta_0) = out'(s_{l_1}, \pi_{s_{l_2}, dom(c_{s_{l_2}})}(c_s), \delta_0)$，记为 $dom(c_{s_{l_2}}), s_{l_2} :| s_{l_1}$。

综上，L 模块内部是无干扰安全的；同理，单向网络安全设备内部各单个模块都满足无干扰性。

b)对于整个网关内部模块的串形复合 [18]，以模块 L、F_1 为例，如图 7 所示。

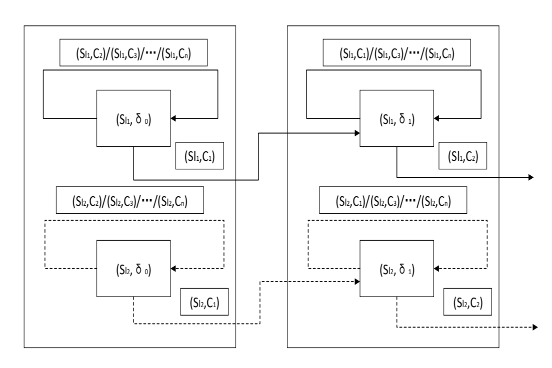


图 7　复合串行模块间信息流动

由无干扰定理可知，若 s_{l_1}, s_{l_2} 是两个不同的主/客体且 $level(s_{l_1}) < level(s_{l_2})$，令所有与 s_{l_1} 相同级别的主/客体所组成的集合记为 s_{l1}，所有与 s_{l_2} 相同级别的主/客体所组成的集合记为 s_{l2}，设 $Z_1 \subseteq Z$ 是一个命令集合，对于所有由 C^* 中元素组成的序列 c_s 和所有的 $s_{l_i} \in s_{l1}$,若证有 $out^{'}(s_{l1}, c_s, \delta_i) = out^{'}(s_{l1}, \pi_{s_{l2},Z_1}(c_s), \delta_i)$。则等价于证明 s_{l2} 中的用户在运行 Z_1 中的命令是不干扰 s_{l1} 中的用户（记为 $Z_1, s_{l2} :| s_{l1}$）。

现证 $Z_1, s_{l2} :| s_{l1}$ 即可。

证明　由上可知，此时 $Z_1 \subseteq dom(c_{s_{l2}})$ 且 $i=0$，即证 $out^{'}(s_{l1}, c_s, \delta_0) = out^{'}(s_{l1}, \pi_{s_{l2},Z_1}(c_s), \delta_0)$ 即可。

采用数学归纳法，令 $\|c_s\|$ 为 c_s 中命令的个数。

（1）基础步：

<1> $\|c_s\| = 0$ 时,上式显然成立;

<2> $\|c_s\| = 1$ 时，即:① $c_s = c_0$,上式成立;

②若 $c_s = (s_{l_j}, c_i)$（j 取正整数），$s_{l_j} \in s_{l1}$，则 $\|Z_1\| = 0$，显然可得 $out^{'}(s_{l1}, \pi_{s_{l2},Z_1}(c_s), \delta_0) = out^{'}(s_{l1}, c_s, \delta_0)$，即:上式成立（$j$ 取正整数）;

③若 $c_s = (s_{l_k}, c_i)$（k 取正整数），$s_{l_k} \in s_{l2}$，有 $Z_1 = (s_{l_k}, c_i)$，可得 $out^{'}(s_{l1}, c_s, \delta_0) = out^{'}(s_{l1}, tra((s_{l_k}, c_i), \delta_0))$ $= out^{'}(s_{l1}, \delta_0)$，而 $out^{'}(s_{l1}, \pi_{s_{l2},Z_1}(c_s), \delta_0) = out^{'}(s_{l1}, \delta_0)$，则上式成立。

（2）假设步：$\|c_s\| \le n$ 时 $out^{'}(s_{l1}, c_s, \delta_0) = out^{'}(s_{l1}, \pi_{s_{l2},Z_1}(c_s), \delta_0)$ 也成立。

（3）归纳步：$\|c_s\| = n+1$ 时，

<1>若 $out^{'}(s_{l1}, c_s, \delta_0) = out^{'}(s_{l1}, c_{s\text{-}1}, T((s_{l_j}, c_i), \delta_0))$ 时，

①当 $i=1$ 时，$tra((s_{l_j}, c_1), \delta_0) = \delta_1$，

令 $out(s_{l1}, c_{s\text{-}1}, \delta_0) = m$（$m$ 为正整数），则：$out(s_{l1}, c_s, \delta_0) = m\text{-}1$,且对于 $out^{'}(s_{l1}, c_{s\text{-}1}, \delta_0)$ 由假设步 (2) 可知：$out^{'}(s_{l1}, c_{s-1}, \delta_0) = out^{'}(s_{l1}, \pi_{s_{l2},Z_1}(c_{s-1}), \delta_0)$，即：$out(s_{l1}, \pi_{s_{l2},Z_1}(c_{s-1}), \delta_0) = m$，∵ $s_{l_j} \notin s_{l2}$ 且 $(s_{l_j}, c_1) \notin Z_1$，

∴ $out(s_{l1}, \pi_{s_{l2},Z_1}(c_s), \delta_0) = m-1$。得: $out(s_{l1}, c_s, \delta_0) = out(s_{l1}, \pi_{s_{l2},Z_1}(c_s), \delta_0)$，

结合假设步(2)有：$out^{'}(s_{l1}, c_s, \delta_0) = out^{'}(s_{l1}, \pi_{s_{l2},Z_1}(c_s), \delta_0)$，证毕;

②当 $i \ne 1$ 时, $tra((s_{l1}, c_i), \delta_0) = \delta_0$。

$out(s_{l1}, c_{s-1}, tra((s_{l_j}, c_i), \delta_0)) = out^{'}(s_{l1}, c_{s-1}, \delta_0)$，结合 (2) 中假设步可得：$out^{'}(s_{l1}, c_{s-1}, \delta_0) = out^{'}(s_{l1}, \pi_{s_{l2},Z_1}(c_{s-1}), \delta_0)$，

∵ $s_{l_j} \in s_{l1}$ 且 $(s_{l_j}, c_i) \notin Z_1$，∴ $out^{'}(s_{l1}, \pi_{s_{l2},Z_1}(c_{s-1}), \delta_0) = out^{'}(s_{l1}, \pi_{s_{l2},Z_1}(c_s), \delta_0)$。即：$out^{'}(s_{l1}, c_{s-1}, tra((s_{l_j}, c_i), \delta_0)) = out^{'}(s_{l1}, c_{s-1}, \delta_0) = out^{'}(s_{l1}, \pi_{s_{l2},Z_1}(c_{s-1}), \delta_0)$ $= out^{'}(s_{l1}, \pi_{s_{l2},Z_1}(c_s), \delta_0)$，

证毕;

<2>若 $out^{'}(s_{l1}, c_s, \delta_0) = out^{'}(s_{l1}, c_{s-1}, tra((s_{l_k}, c_i), \delta_0))$ 时,

∵ $tra((s_{l_k}, c_i), \delta_0) = \delta_0$，∴ $out(s_{l1}, c_{s-1}, tra((s_{l_k}, c_i), \delta_0)) = out^{'}(s_{l1}, c_{s-1}, \delta_0)$。

由假设步可得：$out^{'}(s_{l1}, c_{s-1}, \delta_0) = out^{'}(s_{l1}, \pi_{s_{l2},Z_1}(c_{s-1}), \delta_0)$。

又∵ $(s_{l_k}, c_i) \in Z_1$，∴ $out^{'}(s_{l1}, \pi_{s_{l2},Z_1}(c_{s-1}), \delta_0) = out^{'}(s_{l1}, \pi_{s_{l2},Z_1}(c_s), \delta_0)$。

即：$out^{'}(s_{l1}, c_s, \delta_0) = out^{'}(s_{l1}, \pi_{s_{l2},Z_1}(c_s), \delta_0)$，

证毕。

综上原命题成立，s_{l2} 中的用户在运行 $dom(c_{s_{l2}})$ 中的命令是不干扰 s_{l1} 中的用户（记为 $dom(c_{s_{l2}}), s_{l2} :| s_{l1}$）。同理可得：若单向网络安全设备内部模块间串行连接,当不同级别的信息传递时,单向网络安全设备内部系统是无干扰安全的。

显然，由上已证明出这一模型中任何用户的输出集都与该用户可见的输入集相关，则表明系统 X 关于策略 r 是无干扰安全的。类似的，可以得出结论：如图 2 所示的通信系统此时也是无干扰安全的。

3　隐通道问题及其改进

当出现同级别信息在单向设备内部传递时，对于单个模块信息传递而言系统安全显而易见，现仅考虑模块复合情形，经推理分析发现存在泄密行为（隐通道）。隐通道是一种通信通道，但它不是系统设计者用来通信的信道，因而它能绕过系统强制安全机制[19-20]检查，使得进程能以违反系统安全策略的方式传递信息，从而对系统的安全造成威胁。

3.1　内部隐通道

通常单向网络安全设备内部存在同级别模块的复合，在实际信息传递过程中都存在缓冲区 CR（cache region），不失一般性，以外网通信模块 L 和过滤器模块 F_1 间的消息传递为例。

图 8 中，缓冲区 CR 连接外网通信模块 L 与数据过滤模块 F_1，在模块 L 内部，s_{l1} 为相同级别主/客体信息的信息包，由 $s_{l_1}, s_{l_2} \in s_{l1}$，有 $level(s_{l_1}) = level(s_{l_2})$。$B_l$ 为复合后的输出缓冲区，任何用户都可以读该缓冲区。B_{f_1} 为复合后的输出缓冲区，接收模块 F_1 的输入。CR_1 为主体 s_{l_1} 信息从模块 L 到模块 F_1 的缓冲区，CR_2 为主体 s_{l_2} 信息从模块 L 到模块 F_1 的缓冲区，主体 s_{l_1} 和 s_{l_2} 可以向对应的缓冲区进行写操作，F_1 可以从这些缓冲区读取信息，主体 s_{l_1} 和 s_{l_2} 都可以写缓冲区 CR_{12}，而 F_1 可以读这个缓冲区。如图 8 描述了这种复合。

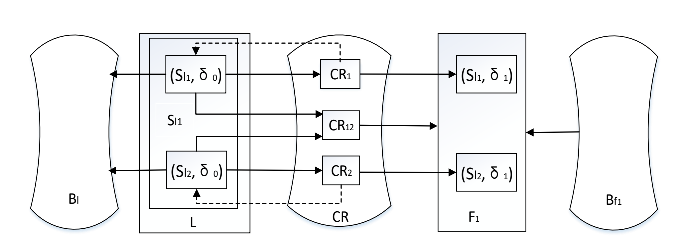


图 8　同级别信息包流动

如果所有缓冲区的长度都是有限的，并且使用阻塞式[21]的发送与接收。不失一般性，假设缓冲区 CR_1 和 CR_2 的长度都是 1，s_{l_1} 循环地执行算法 I：

1.主体 s_{l_1} 发一个消息给 CR_1。使之填满缓冲区；

2.主体 s_{l_1} 给 CR_1 发第二个消息；

3.主体 s_{l_1} 给缓冲区 B_l 发一个 0；

4.主体 s_{l_1} 给 CR_{12} 发一个消息，告诉模块 F_1，主体 s_{l_1} 已经完成了一次循环。

主体 s_{l_2} 也使用相同的算法，但是它用的是 CR_2 而不是 CR_1，并且写一个 1 到 B_l，并记该算法为 $I^{'}$。

模块 F_1 在 B_{f_1} 中读一个比特，如果从 B_{f_1} 中读到的是 0，然后从 CR_1 中收一个消息，或如果从 B_{f_1} 中读到的是 1，然后从 CR_2 中收一个消息，最后从中 CR_{12} 收消息（使得该缓冲区可再次被填满）。

具体分析如下：

在模块 L 向模块 F_1 传递消息时，主体 s_{l_1} 和 s_{l_2} 分别执行各算法第一步，若模块 F_1 在 B_{f_1} 中读到一个 0，主体 S_{l_1} 完成上述算法的后续，而缓冲区 B_l 中也被写入了一个 0；同理，若模块 F_1 在 B_{f_1} 中读到一个 1，主体 s_{l_2} 完成上述算法的后续，而缓冲区 B_l 中也被写入了一个 1。即：模块 F_1 读到的的信息将被一一复制于缓冲区 B_l 中，高级别模块信息通过隐通道（如图虚线所示）流入低级模块，此时单向网络安全设备内部系统是不安全的。

在上述实例中，有限长度并且使用阻塞式发送与接收的缓冲区充当了泄密的隐通道，为了防止这一现象的泄密，提出以下改进方案（即策略完备性[22-23]），如图 9 所示：

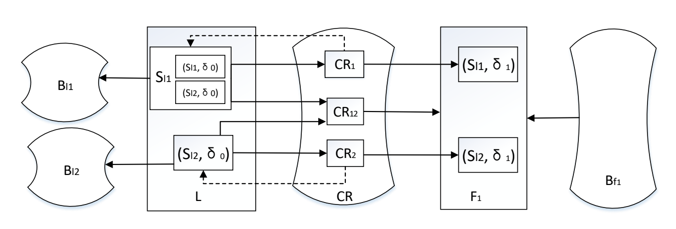


图 9　模块复合时信息流动

每个同级别主体信息所构成的信息包在相邻模块间传递时仅经过一个缓冲区，如图 9 所示，信息包 s_{l1} 和 s_{l2} 有 $level(s_{l2})>level(s_{l1})$，则两信息包的输出缓冲区为 B_{l1}，B_{l2}（$level(B_{l1})<level(B_{l2})$）。

不失一般性，将 $(s_{l1},\delta_0),(s_{l2},\delta_0)$ 当成一个信息包集合，$(s_{l_1},\delta_0),(s_{l_2},\delta_0)\subseteq(s_{l1},\delta_0)$，则令信息包 (s_{l1},δ_0) 内 (s_{l_1},δ_0)、(s_{l_2},δ_0) 等子集循环的执行算法 I，信息包 (s_{l2},δ_0) 内子集循环的执行算法 $I^{'}$。

若子信息包的大小和对应的缓冲区大小恰好一致，此时，在模块 L 向模块 F_1 传递消息时，信息包 (s_{l_1},δ_0) 执行算法 I 第一步，且信息包 (s_{l_k},δ_0)（$(s_{l_k},\delta_0)\in(s_{l2},\delta_0)$）执行算法 $I^{'}$ 第一步，若模块 F_1 在 B_{f_1} 中读到一个 0，主体 s_{l_1} 完成上述算法的后续，信息包 (s_{l_2},δ_0) 被写入缓冲区 CR_1，缓冲区 B_{l1} 中也被写入了一个 0；同理，若模块 F_1 在 B_{f_1} 中读到一个 1，主体 s_{l_2} 完成上述算法的后续，而缓冲区 B_{l2} 中也被写入了一个 1。因为 $level(B_{l1})<level(B_{l2})$，所以缓冲区 B_{l1} 和 B_{l2} 被隔离，主体 s_{l_1} 无法读取缓冲区 B_{l1} 和 B_{l2}，此时系统是安全的。

综上，当单向网络安全设备内部各个模块间采用串行连接且各模块内部同级别主/客体信息信息包仅有一个与之对应的缓冲区时，该单向网络安全设备内部系统是安全的。

3.2　通信系统安全性

现考虑由发送端、单向网络安全设备、接收端所构成的整体系统安全性[24-26]。不失一般性，可以假设出几种不同级别用户信息在系统中的传递路径，如图 10 所示。

图中 $L_{_PC1}$、$L_{_PC2}$、$L_{_PC3}$ 分别为低保密级别网络端 $L_{_D}$ 的用户且 $level(L_{_PC1})=level(L_{_PC2})<level(L_{_PC3})$，$H_{_PC1}$ 和 $H_{_PC2}$ 分别为高保密级别网络端 $H_{_D}$ 接受来自 $L_{_PC1}$、$L_{_PC2}$ 和 $L_{_PC3}$ 信息的用户且 $level(H_{_PC1})<level(H_{_PC2})$，通信模块 A,B,C,D,F 分别由通信模块串行构成的集合（简称通信串集）且 $A\cap B\cap C\cap D\cap F=\varnothing$。

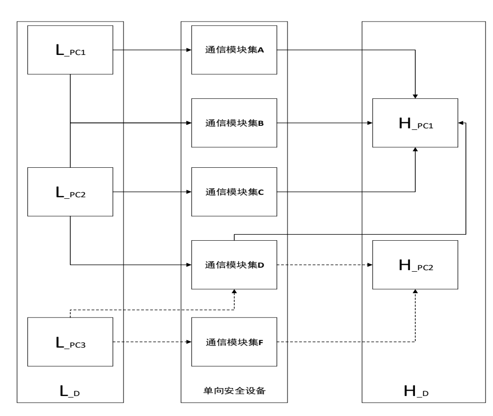


图 10　信息传递图

由第 4.1 节的分析结论，可知图 10 中的个别信息流动的协作会使得整个通信系统处于非安全状态，所以必须作出如下策略改进以使得单向网络安全设备达到预期的安全效果,如图 11 所示.

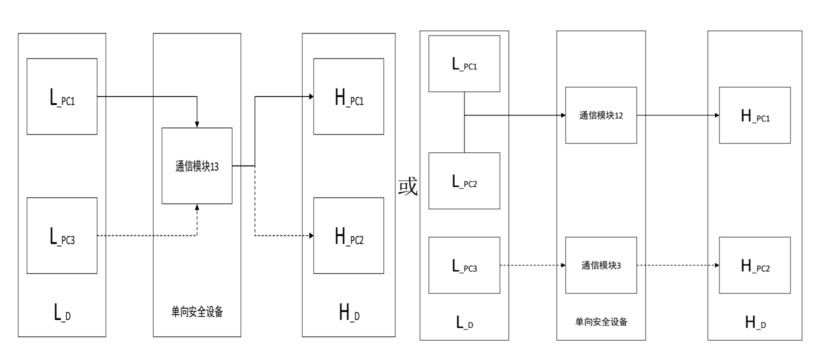


图 11　改进后信息传递图

即单向网络安全设备内部仅含有一个通信串集或同保密级别网络端内同级别用户仅由一特定通信串集处理。信息在此结构传递时整体通信系统是安全的。

4 结束语

在传统意义上，人们经常依靠自身经验去设计单向网络安全设备，其自身的安全性难以就阐述。本文利用无干扰模型形式化分析与讨论单向网络安全设备的安全性，并通过严格的数学证明确定其完备的安全策略。得出如下结论：a）在单向网络安全设备内部，各个通信模块间采用串行连接，且各模块内部同级别主/客体信息信息包仅有一个与之对应的缓冲区时，单向网络安全设备是安全的；b）若发送端、单向网络安全设备、接收端所构成整个通信系统是安全的，则单向网络安全设备内部仅含有一个通信串集或者发送端内同级别用户仅由一个特定通信模串集处理。由此可见，这种设计所存在明显缺陷，对同级别用户来说，等待同一同信模块的处理是耗时的，所以应考虑使得单向网络安全设备内部通信模块处理能力远大于读取能力。

后面的工作当中，将对单向网络安全设备中各个模块内部信息的复合传递进行进一步细化及其分类，利用形式化分析方法和数学工具近一步证明各模块内部的行为与其代码一致性，从而得到一个经过严格完整证明的单向网络安全设备。

参考文献：

[1] Chapman D B. Building Internet firewalls [M]. 北京：清华大学出版社, 2003.

[2] Phifer L. Simplifying secure remote access: SSL VPNs [C]// Proc of Business Communications Review. 2003.

[3] Comer D E. Internelworking with TCP//IP [C]// Proc of IEEE Symposium on Computers and Communications. [S. l.] : IEEE Computer Society, 1995: 255.

[4] 叶盛，高海锋，张根度. VPN 的实现机制和系统评价 [J]. 小型微型计算机系统, 2002, 23 (9): 1053-1058.

[5] 熊蔚明，刘有恒. 关于通信网可靠性的研究进展 [J]. 通信学报, 1990 (4): 43-49.

[6] Tolstrup T K, Nielson F, Hansen R R. Locality-based security policies [C]// Lecture Notes in Computer Science. 2007: 185-201.

[7] 周权，肖德琴，唐屹. 基于 Linux 和 IPSec 的 VPN 安全网关设计与实现 [J]. 计算机应用研究, 2005, 22 (9): 229-231, 234.

[8] MattBishop. 计算机安全学：安全的艺术与科学 [M]. 北京：电子工业出版社, 2005.

[9] Denning D E. A lattice model of secure information flow [J]. Communications of the ACM, 1976, 16 (5): 236-243.

[10] Bell D E, Lapadula L J. Secure computer systems: mathematical foundations [C]// Proc of Cornputer Secilrity Formdations Workshop. 1973.

[11] Goguen J A, Meseguer J. Security policies and security models [C]// Proc of IEEE Symposium on Security & Privacy. 1982: 11-20.

[12] Rossum P V, Rossum P V, Smith G. Computing the leakage of information-hiding systems [C]// Proc of International Conference on TOOLS and Algorithms for the Construction and Analysis of Systems. [S. l.] : Springer-Verlag, 2010: 373-389.

[13] Askaro A, Chong S, Mantel H. Hybrid monitors for concurrent noninterference [C]// Proc of IEEE Computer Security Foundations Symposium. 2015: 137-151.

[14] Alvim M S, Chatzikokolakis K, Palamidessi C, et al. Measuring information leakage using generalized gain functions [C]// Proc of IEEE Computer Security Foundations Symposium. 2012: 265-279.

[15] Goguen J A, Meseguer J. Unwinding and inference control [C]// Proc of IEEE Symposium on Security and Privacy. 1984: 75-75.

[16] Mclean J. Proving noninterference and functional correctness using traces [J]. Journal of Computer Security. 1992, 1: 37-58.

[17] Forster R. Non-interference properties for nondeterministic processes [D]. [S. l.] : University of Oxford, 1999.

[18] Rafnsson W, Jia L, Bauer L. Timing-sensitive noninterference through composition [C]// Proc of International Conference on the Principles of Security and Trust. 2017.

[19] Barthe G, Kopf B. Information-theoretic bounds for differentially private mechanisms [C]// Proc of IEEE Computer Security Foundations Symposium. 2014: 191-204.

[20] Biondi F, Kawamoto Y, Legay A, et al. HyLeak: hybrid analysis tool for information leakage [C]// Proc of International Symposium on Automated Technology for Verification and Analysis. Cham: Springer, 2017: 156-163.

[21] Yasuoka H, Terauchi T. Quantitative information flow-verification hardness and possibilities [C]// Proc of IEEE Computer Security Foundations Symposium. [S. l.] : IEEE Computer Society, 2010: 15-27.

[22] Chothia T, Kawamoto Y. Statistical estimation of min-entropy leakage [Z]. 2014.

[23] Focardi R, Gorrieri R, Martinelli F. Non interference for the analysis of cryptographic protocols [C]// Proc of International Colloquium on Automata, Languages and Programming. [S. l.] : Springer-Verlag, 2000: 354-372.

[24] Mccullough D. Noninterference and the composability of security properties [C]// Proc of IEEE Symposium on Security and Privacy. 1988: 177-186.

[25] Bevier W R, Young W D. A state-based approach to noninterference [C]// Proc of IEEE Computer Security Foundations Workshop. 1994: 11-21.

[26] Johnson D M, Thayer F J. Security and the composition of machines [C]// Proc of the 1st IEEE Computer Security Foundations Workshop. 1988: 72-89.